Unitarily Graded Field Extensions

Holger Brenner, Almar Kaid and Uwe Storch

Abstract

We introduce the universal unitarily graded A-algebra $A\langle U\rangle$ for a commutative ring A and an arbitrary extension $A^\times \hookrightarrow U$ of abelian groups (where $A^\times$ denotes the group of units of A) and use this concept to give among other things simplified and concise proofs of the main theorems of the so called co-Galois theory described in the book "Cogalois Theory" by T. Albu. The main tool is a generalisation of a theorem by M. Kneser which, in our language, is a criterion for $A\langle U\rangle$ to be a field under the obvious assumption that the base ring A is itself a field and that $A\langle U\rangle$ is separable (and algebraic) over A. This theorem implies also the theorem of A. Schinzel on linearly independent roots. Since essential group extensions $A^\times \hookrightarrow U$ play a fundamental role we discuss examples involving the injective hull of the multiplicative group of a field. Furthermore,we develop criteria for Galois extensions which allow a co-Galois grading, in particular for the cyclic case.

Mathematical Subject Classification (2000): 11R32; 11R20; 12F10; 12E30; 13A02

1. Introduction

Throughout this paper we will consider only commutative rings. First of all we fix some notations which we will use consistently: $\mathbb{P}$ denotes the set of all prime numbers in $\mathbb{N}^* = \mathbb{N}\setminus\{0\}$. For an abelian group G with a multiplicatively written operation and a prime number p we denote by $G[p^\infty] := \{x \in G : x^{p^k} = 1, k \geq 1\}$ the *p-primary component* and by $G[p] := \{x \in G : x^p = 1\}$ the *p-socle* of G. The *order* of G is denoted by $|G|$ or $\operatorname{ord}(G)$ and its *exponent* by $\exp(G)$. The order of an element x of a group is denoted by $\operatorname{ord} x (\in \mathbb{N})$. We write $A^\times$ for the group of units of a ring A and $\mu_n(A) := \{x \in A^\times : x^n = 1\}$ for the group of n-th roots of unity in A, $n \in \mathbb{N}^*$. For a field K the group $\mu_n(K) \subseteq K^\times$ is cyclic. By ζ_n we always denote a *primitive* root of unity in $K^\times$, i.e. a root of unity of order n. If $K = \mathbb{C}$, we denote by ζ_n the standard root of unity $\exp(2\pi i/n)$. If $K \subseteq L$ is an extension of fields we simply write $L|K$ and denote by $[L : K] := \dim_K L$ the *degree* of L over K. The Galois group $\operatorname{Aut}_{K\text{-alg}} L$ of $L|K$ is denoted by $\mathrm{G}(L|K)$.

In this paper A denotes always a base ring, which is not the zero ring, and D denotes an abelian group with additively written operation.

Definition 1.1. Let $B = \bigoplus_{d\in D} B_d$ be a D-graded A-algebra. Then we call B *unitarily D-graded*, if $B_0 = A$ and $B_d^\times := B_d \cap B^\times \neq \emptyset$ for every $d \in D$.

For a unitarily D-graded A-algebra $B = \bigoplus_{d\in D} B_d$ every homogeneous component B_d, $d \in D$, is obviously a free A-module of rank one. (Notice that in the unitarily graded case $B_d B_e = B_{d+e}$ holds for $d, e \in D$. Hence, unitarily graded algebras are strongly graded algebras in the sense of [3].) In particular, a unitarily D-graded A-algebra is a free A-algebra.

Let $x \in B_d^\times$. Then $x^{-1} \in B_{-d}$, $B_d^\times = A^\times x$ and x is transcendental over A if $d \in D$ is not a torsion element and algebraic over A with minimal polynomial $X^{\operatorname{ord} d} - x^{\operatorname{ord} d}$ else. In particular, a unitarily graded A-Algebra B is integral over A if and only if its grading group is a torsion group.

If $D' \subseteq D$ is a subgroup of D then $B_{D'} := \bigoplus_{d\in D'} B_d$ is obviously a unitarily D'-graded A-subalgebra of B. Moreover, B is unitarily D/D'-graded over $B_{D'}$ with homogeneous components $B_{d+D'} = \sum_{d'\in D'} B_{d+d'} = B_d B_{D'}$ and $B_{d+D'}^\times = B_d^\times B_{D'}^\times$. Conversely, if $C \subseteq B$ is an A-subalgebra of B then one easily checks that $D_C := \{d \in D : B_d^\times \cap C^\times \neq \emptyset\}$ is a subgroup of D.

If B is unitarily D-graded and $D = D_1 \times D_2$ with subgroups $D_1, D_2 \subseteq D$, then the canonical homomorphism $B_{D_1} \otimes_A B_{D_2} \to B = B_D$ is an isomorphism of D-graded rings. If B and B' are unitarily D and D'-graded respectively then $B \otimes_A B' = \bigoplus_{(d,d')\in D\times D'} B_d \otimes_A B_{d'}$ is a unitary $(D \times D')$-grading of $B \otimes_A B'$.

Let B be a unitarily D-graded A-algebra and $A \to A'$ a ring homomorphism. Then $B' := B \otimes_A A'$ is a unitarily D-graded A'-algebra.

Example 1.2. The A-algebra $A[X]/(X^n - a)$, $a \in A^\times$, has a natural unitary $\mathbb{Z}_n$-grading. Hence,

$$A[X_1, \dots, X_r]/(X_1^{n_1} - a_1, \dots, X_r^{n_r} - a_r) = \bigotimes_{j=1}^{r} A[X_j]/(X_j^{n_j} - a_j),$$

$a_1, \dots, a_r \in A^\times$, has a natural unitary $(\prod_{j=1}^r \mathbb{Z}_{n_j})$-grading. Since any finite abelian group is a direct sum of cyclic groups *every finite unitarily graded A-algebra is up to (graded) isomorphism of this type.*

Example 1.3. The group algebra $A[D] = \bigoplus_{d\in D} AT^d$ is obviously a unitarily D-graded A-algebra.

We denote by ${}^hB^\times$ the homogeneous units of a graded ring B, which is obviously a subgroup of $B^\times$. Two unitary gradings are by definition *essentially the same* if their groups of homogeneous units coincide. The map $\deg : {}^hB^\times \to D$, which maps an element $x_d \in B_d^\times$ to its degree d, is a homomorphism of abelian groups. By definition of a unitarily D-graded A-algebra we get the following:

Proposition 1.4. *Let B be a unitarily D-graded A-algebra. Then*

$$1 \longrightarrow A^\times \longrightarrow {}^hB^\times \xrightarrow{\deg} D \longrightarrow 0$$

is an exact sequence of abelian groups. Especially, there is a canonical isomorphism $D \cong {}^hB^\times/A^\times$.

With respect to Proposition 1.4, we often identify the groups D and ${}^{h}B^{\times}/A^{\times}$, but continue to write the operation in D additively.

For an abelian group U containing $A^{\times}$, we construct a universal unitarily $U/A^{\times}$-graded A-algebra in the following way: We denote $U/A^{\times}$ by D and write $d \in D$ for a class $A^{\times}x$. We choose a system $x_d \in U$ of representatives for the elements $d = A^{\times}x_d \in D = U/A^{\times}$ and consider the free A-module

$$A\langle U\rangle := \bigoplus\nolimits_{d\in D} Ax_d$$

with A-basis x_d, $d \in D$. The product x_dx_e for $d, e \in D$ is given by the multiplication in U, i.e. $x_dx_e = a_{d,e}x_{d+e}$ with $a_{d,e} \in A^{\times}$. It is obvious that $A\langle U\rangle$ is a unitarily D-graded A-algebra and that U can be identified with ${}^{h}A\langle U\rangle^{\times}$ via the canonical inclusion $\gamma : U \to A\langle U\rangle^{\times}$, $x \mapsto ax_d$, where $A^{\times}x = A^{\times}x_d$ and $x = ax_d$ with $a \in A^{\times}$. In particular $A\langle U\rangle^{\times}_{d} = A^{\times}x_d$ and for any system $y_d \in U$, $d \in D$, of representatives for $U/A^{\times}$ the elements $\gamma(y_d)$, $d \in D$, form an A-basis of $A\langle U\rangle$.

The pair $(A\langle U\rangle, \gamma)$ has the following universal property (which, by the way, proves its uniqueness):

Proposition 1.5. *Let B be a (not necessarily graded) A-algebra together with a group homomorphism $\psi : U \to B^{\times}$ that coincides on $A^{\times}$ with the structure homomorphism of B. Then there is a uniquely determined A-algebra homomorphism $\bar{\psi} : A\langle U\rangle \to B$ such that $\psi = \bar{\psi} \circ \gamma$.*

Proof. Because the elements x_d form an A-basis of $A\langle U\rangle$ we can extend the group homomorphism ψ to an A-module homomorphism $\bar{\psi} : A\langle U\rangle \to B$ by $\bar{\psi}(x_d) := \psi(x_d)$. Due to the assumption that ψ coincides on $A^{\times}$ with the structure homomorphism of B one easily checks that $\bar{\psi}$ is even an A-algebra homomorphism. □

Remark 1.6. One can define the algebra $A\langle U\rangle$ alternatively as $A \otimes_{B[A^{\times}]} B[U]$, where $B \to A$ is any ring homomorphism (and $B[U]$, $B[A^{\times}]$ are the group algebras). In particular, one can set $A\langle U\rangle := A \otimes_{\mathbb{Z}[A^{\times}]} \mathbb{Z}[U]$. We thank the referee for this useful comment.

Remark 1.7. We can interpret every unitarily graded A-algebra B as such a universal algebra $A\langle U\rangle$ with $U := {}^{h}B^{\times}$. So the algebra structure of B is already determined by the group extension $A^{\times} \hookrightarrow {}^{h}B^{\times}$.

Remark 1.8. It is well known that the group $\operatorname{Ext}(D, A^{\times}) = \operatorname{Ext}^1_{\mathbb{Z}}(D, A^{\times})$ describes the isomorphy classes of exact sequences

$$1 \longrightarrow A^{\times} \longrightarrow U \longrightarrow D \longrightarrow 0$$

of abelian groups. So the group $\operatorname{Ext}(D, A^{\times})$ also classifies the isomorphy types of unitarily D-graded A-algebras. The trivial element of $\operatorname{Ext}(D, A^{\times})$ is the direct product $A^{\times} \times D$ which corresponds to the group algebra $A[D] = A\langle A^{\times} \times D\rangle$.

2. Unitarily graded field extensions

The aim of this section is to give an answer to the following natural question: For which extensions $A^\times \hookrightarrow U$ of abelian groups is the universal algebra $A\langle U\rangle$ a field? If this is the case, necessarily A itself is a field. Therefore, we assume in this section that the base ring A is a field K. Furthermore we use throughout our standard notations: For an extension $K^\times \hookrightarrow U$ of abelian groups $K\langle U\rangle$ is the universal algebra constructed in section 1. It is unitarily graded, its group ${}^hK\langle U\rangle^\times$ of homogenous units can be identified with U and the grading group is $D := U/K^\times$. For every unitarily graded K-algebra B the canonical homomorphism $K\langle {}^hB^\times\rangle \to B$ is an isomorphism. We want to clarify that a unitarily graded field extension $L|K$ is a *Kneser extension* as introduced in [1, Definition 2.1.9 and Definition 11.1.1] and vice versa. Important examples of unitarily graded field extensions are the Kummer extensions.

Example 2.1. We recall that a (not necessarily finite) algebraic field extension $L|K$ is a *Kummer extension*, if $L|K$ is a Galois extension with abelian Galois group $\mathrm{G}(L|K)$ and if for every finite intermediate field $K \subseteq E \subseteq L$ the base field K contains a root of unity of order $\exp(\mathrm{G}(E|K))$. The last property is fulfilled if and only if the group of all continuous characters $\check{\mathrm{G}}(L|K) := \mathrm{Hom}(\mathrm{G}(L|K), \mathbb{Q}/\mathbb{Z})$ can be identified with the group of the (continuous) characters $\mathrm{G}(L|K) \to K^\times$ with values in $K^\times$.

Proposition 2.2. (1) *Let $L|K$ be a Kummer extension with Galois group $G := \mathrm{G}(L|K)$. For a* (*continuous*) *character $\chi : G \to K^\times$ let L_χ denote its eigenspace $L_\chi := \{x \in L : \sigma(x) = \chi(\sigma)x \text{ for all } \sigma \in G\}$. Then $L = \bigoplus_{\chi\in\check{G}} L_\chi$ is a unitary $\check{G}$-grading of L over K, $\check{G} = \mathrm{Hom}(G, K^\times)$.*

(2) *Conversely, let $L = \bigoplus_{d\in D} L_d$ be a unitarily D-graded field extension of $K = L_0$ and suppose that K contains a root of unity of order n_0 whenever D contains an element of order n_0. Then L is a Kummer extension of K with Galois group $\check{D} = \mathrm{Hom}(D, K^\times)$, where a character $\delta : D \to K^\times$ operates as $\delta(\sum_{d\in D} x_d) = \sum_{d\in D} \delta(d)x_d$.* (*Here a character $\delta \in \check{D}$ is an* arbitrary *group homomorphism $D \to K^\times$, and the topology of $\check{D}$ as a profinite group is given by the finite subgroups $D_0 \subseteq D$ with the surjections $\check{D} \to \check{D}_0$, $\check{D} = \varprojlim \check{D}_0$.*) *Especially, L_d is necessarily the eigenspace for the character $\chi_d : \check{D} \to K^\times$, $\delta \mapsto \delta(d)$, and the given grading of L can be identified with the grading of part* (1). *Furthermore, the only intermediate fields of $L|K$ are the graded fields $L_{D'}$, D' subgroup of D.*

Proof. One reduces easily both assertions to the case of a finite extension $L|K$. For part (2) note that the grading group D is necessarily a torsion group by Proposition 2.3 below.

(1) Then, by the assumption on the roots of unity in K, every K-linear operator $\sigma \in G$ of L is diagonalisable over K. Since G is commutative the elements of G are simultaniously diagonalisable, i.e. $L = \bigoplus_{i\in I} L_i$ with G-invariant 1-dimensional K-subspaces $L_i \subseteq L$. Trivially, for every $i \in I$ the function $\chi : G \to K^\times$ with $\chi(\sigma) = \sigma(x)x^{-1}$ for all $\sigma \in G$ and all $x \in L_i\setminus\{0\}$ is a character. Because of $|\check{G}| = |G| = [L : K]$, and $L_\chi L_{\chi'} \subseteq L_{\chi\chi'}$, it suffices to show that $\dim_K L_\chi \le 1$ for all $\chi \in \check{G}$, but $L_1 = K$ for the trivial character 1 and $L_\chi = L_1 x$ for any $x \in L_\chi\setminus\{0\}$.

(2) Obviously, $\delta : L \to L$ is a K-automorphism of L, which respects the grading. Because of $|D| = |\check{D}| = [L : K]$ these are all K-automorphisms of L. □

Let us mention that a Kummer extension $L|K$ may have unitary gradings which are essentially different from the canonical grading described in Proposition 2.2. For instance, the cyclotomic field $\mathbb{Q}[\zeta_8] = \mathbb{Q}[i, \sqrt{2}] \cong \mathbb{Q}[X]/(X^4 + 1) \cong \mathbb{Q}[Y, Z]/(Y^2 + 1, Z^2 - 2)$ is a Kummer extension of $\mathbb{Q}$ which has besides the canonical $\mathbb{Z}_2 \times \mathbb{Z}_2$-grading a unitary $\mathbb{Z}_4$-grading. The canonical grading of a Kummer extension $L|K$ is characterised by the property that the base field K contains a root of unity of order n_0 if the grading group D contains an element of order n_0, $n_0 \in \mathbb{N}^*$.

Proposition 2.3. *Let $L = K\langle U\rangle$ be a field. Then the group extension $K^\times \hookrightarrow U$ is essential and, in particular, the grading group $D = U/K^\times$ is a torsion group.*

Proof. To prove that D is a torsion group let $d_0 \in D$, $d_0 \neq 0$, and $x_{d_0} \in L^\times_{d_0}$. Then $1 + x_{d_0} \in L^\times$. Let $\sum_{d\in D} y_d$ be the inverse of $1 + x_{d_0}$. The equation $(1 + x_{d_0}) \sum_{d\in D} y_d = 1$ implies $y_0 = 1 - x_{d_0} y_{-d_0}$ and $y_d = -x_{d_0} y_{d-d_0}$ for all $d \neq 0$. The first equation implies $y_0 \neq 0$ or $y_{-d_0} \neq 0$. The other equations imply (by induction) $y_{kd_0} = (-1)^k x^k_{d_0} y_0$ for all $k \in \mathbb{Z}$, hence $y_{kd_0} \neq 0$ for all $k \in \mathbb{Z}$. It follows that $\mathbb{Z}d_0$ is a finite group.

We want to recall that an extension $H \subseteq G$ of abelian groups is by definition *essential*, if for every subgroup $F \subseteq G$ with $F \cap H = 1$ already $F = 1$ holds. It is easy to prove that this is equivalent to the following conditions: The quotient G/H is a torsion group and, for every prime number p, the p-socles $H[p]$ and $G[p]$ coincide. In our case $H = K^\times$ is the multiplicative group of the field K. Therefore, the extension $K^\times \subseteq U$ is essential if and only if $U/K^\times$ is a torsion group and every root of unity of order p, $p \in \mathbb{P}$, in U belongs already to $K^\times$.

The quotient $U/K^\times = D$ is a torsion group by the first part. Assume ζ_p is a root of unity of order p, $p \in \mathbb{P}$, in ${}^hL^\times \setminus K^\times$. Then the graded K-subalgebra $K[\zeta_p] \cong K[X]/(X^p - 1)$ is not a field. Contradiction. □

Proposition 2.3 says in particular, that a unitarily graded field extension $L|K$ is algebraic. A homogeneous element $x_d \in L^\times_d$, $d \in D \cong {}^hL^\times/K^\times$, has degree $\operatorname{ord} d$ over K. Therefore, L is separably algebraic if and only if $\operatorname{char} K = 0$ or $\operatorname{char} K = \ell > 0$ and $D[\ell^\infty] = 0$.

Since we are only interested in the separable case, from now on *we presuppose in this section that $U/K^\times$ is a torsion group and that $(U/K^\times)[\ell^\infty] = 1$ in case* $\operatorname{char} K = \ell > 0$.

The following three lemmas are the essential steps for the proof of the main theorem.

Lemma 2.4. *Let $D = U/K^\times$ be a finite p-group of order p^α, $\alpha \geq 1$, p prime ($\neq \operatorname{char} K$). In case $p = 2$ assume $i = \sqrt{-1} \in K$. Then $B := K\langle U\rangle$ is a field if and only if the group extension $K^\times \hookrightarrow U$ is essential. – In this case $(B^\times/K^\times)[p^\infty] = U/K^\times = {}^hB^\times/K^\times = D$.*

Proof. By Proposition 2.3 the extension $K^\times \hookrightarrow U$ is essential if B is a field. For the proof of the converse and the supplement we use induction on α. Let $\alpha = 1$. Then $B = K[x] \cong K[X]/(X^p - a)$ where $x \in U \setminus K^\times$ and $a = x^p \in K^\times$. We have to show that the polynomial $X^p - a$ is irreducible. Assume that $X^p - a$ has a zero y in a field extension L of K of degree $m < p$. Then $a = y^p$ and $a^m = \mathrm{N}_K^L(a) = \mathrm{N}_K^L(y)^p$ (where N_K^L denotes the norm function). Because of $\gcd(m,p) = 1$ we have $a = b^p$ with $b \in K^\times$ and $(x/b)^p = 1$ with $x/b \in U$. It follows $x/b \in K^\times$ (since $K^\times \hookrightarrow U$ is essential) and $x \in K^\times$. Contradiction.

To prove the supplement it is enough to show: If $y \in B^\times$ and $y^p \in U = {}^hB^\times$ then $y \in U$. We adjoin if necessary to K a root of unity ζ_p of order p and consider the Kummer extension $K[\zeta_p] \subseteq K[\zeta_p] \otimes_K B = B[\zeta_p] \cong K[\zeta_p][X]/(X^p - a)$. (Note that $K[\zeta_p] \otimes B$ is a field because of $\gcd([K[\zeta_p] : K], [B : K]) = 1$.)

First assume that even $y^p \in K^\times$. If $y \notin K^\times$ then $B = K[y]$ and $B[\zeta_p] = K[\zeta_p][y]$. By Proposition 2.2 the element y is homogeneous in $B[\zeta_p]$ (since $K[\zeta_p]y^k$, $k = 0, \dots, p-1$, are the homogeneous components of a unitary grading of $B[\zeta_p]$). Then y is homogeneous in B too, i.e. $y \in U$.

Now suppose $y^p \notin K^\times$. Then $y^{p^2} = (y^p)^p =: c \in K^\times$ and $X^p - c$ is the minimal (= characteristic) polynomial of y^p and $c = (-1)^{p+1}\,\mathrm{N}_K^B(y^p) = (-1)^{p+1}\,\mathrm{N}_K^B(y)^p$. In any case c is a p-th power in $K^\times$ (in case $p = 2$ we use $i \in K$). This contradicts the irreducibility of $X^p - c$.

For the induction step assume $|D| = p^{\alpha+1}$. Let $\tilde{D} \subset D$ be a subgroup of order p^α. Then by induction hypothesis, the unitarily $\tilde{D}$-graded subalgebra $\tilde{B} := B_{\tilde{D}} \subset B$ is a field with $(\tilde{B}^\times/K^\times)[p^\infty] = {}^h\tilde{B}^\times/K^\times$ and B is a unitarily $D/\tilde{D}$-graded $\tilde{B}$-algebra with $\tilde{B}^\times {}^hB^\times$ as group of homogeneous units. The group extension $\tilde{B}^\times \hookrightarrow \tilde{B}^\times {}^hB^\times$ is essential. To prove this, let $(yz)^p = y^p z^p = 1$, $y \in \tilde{B}^\times$, $z \in {}^hB^\times$. Then $z^p \in {}^h\tilde{B}^\times$, $y^p \in {}^h\tilde{B}^\times$, so $y \in {}^h\tilde{B}^\times$ by the induction hypothesis on the supplement. Hence $yz \in {}^hB^\times$ and $yz \in K^\times \subseteq \tilde{B}^\times$ since $K^\times \hookrightarrow {}^hB^\times$ is essential. The case $\alpha = 1$ implies that B is a field and $(B^\times/\tilde{B}^\times)[p^\infty] = \tilde{B}^\times {}^hB^\times/\tilde{B}^\times$.

To prove $(B^\times/K^\times)[p^\infty] = {}^hB^\times/K^\times$ let $w \in B^\times$ represent an element in $(B^\times/K^\times)[p^\infty]$. Then $w \in \tilde{B}^\times {}^hB^\times$, $w = uv$ with $u \in \tilde{B}^\times$, $v \in {}^hB^\times$, hence $u \in {}^h\tilde{B}^\times$ and $w \in {}^hB^\times$ as wanted. □

Lemma 2.5. *Let $D = U/K^\times$ be a finite 2-group of order 2^α, $\alpha \geq 1$. Assume U contains no element of order 4. Then $B := K\langle U \rangle$ is a field if and only if the group extension $K^\times \hookrightarrow U$ is essential. – In this case $(B^\times/K^\times)[2^\infty] = U/K^\times = {}^hB^\times/K^\times = D$.*

Proof. By Proposition 2.3 the extension $K^\times \hookrightarrow U$ is essential if B is a field. We consider the extension $K[i] \subseteq B[i] := K[i] \otimes_K B$. It is enough to show that the extension $K[i]^\times \hookrightarrow {}^hB[i]^\times$ is essential. Then, due to 2.4, $B[i]$ is a field hence B too. Furthermore, $(B[i]^\times/K[i]^\times)[2^\infty] = {}^hB[i]^\times/K[i]^\times$ which implies $(B^\times/K^\times)[2^\infty] = {}^hB^\times/K^\times$ because of ${}^hB^\times = {}^hB[i]^\times \cap B$. We have $B[i]_d = B_d \oplus B_d i$ for all $d \in D$. So let $b, c \in B_d$ with $1 = (b + ci)^2 = b^2 + 2bci - c^2$. Comparison of coefficients yields $b^2 - c^2 = 1$ and $2bc = 0$.

Because char $K \neq 2$ we have $b = 0$ or $c = 0$. Suppose $b = 0$, hence $-c^2 = 1$. But this means $c = \pm i \in {}^hB^\times$ which is a contradiction. So we have $c = 0$, hence $b^2 = 1$. Because $K^\times \subseteq {}^hB^\times$ is essential we get $b = \pm 1$. □

Note that in the situation of Lemma 2.4 or Lemma 2.5 the torsion group $\mathrm{t}(B^\times/K^\times)$ may be larger than $U/K^\times = {}^hB^\times/K^\times$ even if B is a field! A simple example is $B = \mathbb{Q}[\zeta_3] = \mathbb{Q}[\sqrt{-3}]$ over $K = \mathbb{Q}$.

If $D = U/K^\times$ is a finite 2-group the condition that the extension $K^\times \hookrightarrow U$ is essential is in general not sufficient for $K\langle U\rangle$ to be a field. By 2.5 this can only occur if U contains an element of order 4.

Example 2.6. We consider the polynomial $X^4 + 4 \in \mathbb{Q}[X]$. We have the well-known decomposition $X^4+4 = (X^2-2X+2)(X^2+2X+2)$ over $\mathbb{Q}$, so the unitarily $\mathbb{Z}_4$-graded $\mathbb{Q}$-Algebra $B := \mathbb{Q}[X]/(X^4 + 4)$ is not a field. But the extension $\mathbb{Q}^\times \subseteq {}^hB^\times$ is essential due to the fact that there is no element $y \in {}^hB^\times \backslash \mathbb{Q}^\times$ with $y^2 = 1$. The element $x^2/2$ has order 4 in $U = {}^hB^\times$.

Lemma 2.7. *Let $D = U/K^\times$ be a finite 2-group of order 2^α, $\alpha \geq 1$. Assume U contains an element of order 4 which is not an element of K. Then $B := K\langle U\rangle$ is a field if and only if the group extension $K^\times \hookrightarrow U$ is essential and $-4 \notin U^4$ (i.e. there is no element $x \in U$ with $x^4 = -4$).*

Proof. If B is a field then $K^\times \hookrightarrow U$ is essential by Proposition 2.3. Furthermore, if there is an element $x \in U$ with $x^4 = -4$, then x represents an element of order 4 in $D = U/K^\times$ because $(x^2/2)^2 = -1$ and therefore $x^2 = \pm 2i \notin K^\times$ by assumption. It follows $K[x] \cong K[X]/(X^4+4)$, and $K[x]$ is not a field because of $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$, see also Example 2.6.

Conversely, the element $i \in U$ of order 4 represents an element of order 2 in $U/K^\times$ because of $i^2 = -1$. So $K[i] \subseteq B$ is a graded quadratic subfield of B and B is unitarily graded over $K[i]$ with grading group $K[i]^\times U/K[i]^\times$. By Lemma 2.4 it is now sufficient to show that the extension $K[i]^\times \hookrightarrow K[i]^\times U$ is essential. To do this, let $y^2 = x^2$ with $y \in U$, $x = a + bi \in K[i]^\times$, $a, b \in K$. Then $y^2 = a^2 - b^2 + 2abi \in U$, hence $a^2 - b^2 = 0$ or $2ab = 0$. If $a^2 - b^2 = 0$, then $a = \pm b$, $(y/a)^4 = (\pm 2i)^2 = -4$ which is impossible by assumption. Therefore $ab = 0$, i.e. $x \in U$, hence $x^{-1}y \in U$ and $x^{-1}y = \pm 1$ since $K^\times \hookrightarrow U$ is essential. □

Remark 2.8. (1) In the situation of 2.7 it is rather difficult to describe the 2-torsion group $(B^\times/K^\times)[2^\infty]$. Because $1 + i \notin U$ represents an element of order 4 in $B^\times/K^\times$ the group $(B^\times/K^\times)[2^\infty]$ is always larger than ${}^hB^\times/K^\times = U/K^\times$. But the simple example $K := \mathbb{R}$, $B := \mathbb{R}[i] = \mathbb{C}$ shows that $(B^\times/K^\times)[2^\infty]$ can be much larger than $U/K^\times$.

(2) It would be interesting to understand the structure of the separable K-algebra $B = K\langle U\rangle$ or at least its spectrum if the essential extension $K^\times \hookrightarrow U$ fulfills all the assumptions of Lemma 2.7 and moreover $-4 \in U^4$. For illustrations look at Example 2.6 and its extension Example 3.10 in the next section or at the following one: For K take the real number field $\mathbb{Q}[\zeta_{16}] \cap \mathbb{R}$ and for U the essential extension $K^\times\mu_{16}(\mathbb{C})$ of $K^\times$ with $K^\times\mu_{16}(\mathbb{C})/K^\times \cong \mathbb{Z}_8$. Then $1 + i = \sqrt{2}\,\zeta_8 \in U$

with $(1+i)^4 = -4$ and $K\langle U\rangle \cong K \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_{16}]$ splits into 4 components which are isomorphic quadratic field extensions of K.

The comments in this remark also show that the statements in [7], §93, Exercise 14e)(3),(4) are not correct.

The following theorem which generalises amongst others the Theorem of M. Kneser in [6] is the main result and summarises the results of the previous lemmata, cf. also [5, Satz 3.2.6].

Theorem 2.9. *For the group extension $K^\times \hookrightarrow U$ (with $(U/K^\times)[\ell^\infty] = 1$ if $\operatorname{char} K = \ell > 0$) the universal algebra $K\langle U\rangle$ is a field if and only if the extension $K^\times \hookrightarrow U$ is essential and moreover $-4 \notin U^4$ in case U contains an element of order 4 not in $K^\times$. – In this case $(K\langle U\rangle^\times/K^\times)[p^\infty] = U/K^\times$ if $U/K^\times$ is a p-group, $p \geq 3$, and $(K\langle U\rangle^\times/K^\times)[2^\infty] = U/K^\times$ if $U/K^\times$ is a 2-group and U contains no element of order 4 not in K.*

Proof. Let $D := U/K^\times$. If the unitarily D-graded K-algebra $B := K\langle U\rangle$ is a field then $K^\times \hookrightarrow U$ is essential by 2.3 and the exceptional case is settled by Lemma 2.7 because of $B_{D[2^\infty]} \subseteq B$.

Conversely, let $K^\times \hookrightarrow U$ be essential with $-4 \notin U^4$ in the special case. Because of $K\langle U\rangle = \varinjlim K\langle U'\rangle$ where U' runs through the subgroups $U' \subseteq U$ with $K^\times \subseteq U'$ and finite index $[U' : K^\times]$ we may assume that $D = U/K^\times$ is finite. Then $B = \bigotimes_p B_{D[p^\infty]}$ because of $D = \bigoplus_p D[p^\infty]$, where p runs through the prime divisors of $|D|$. Since the dimensions $\dim_K B_{D[p^\infty]}$ are pairwise coprime it is enough to show that all the K-algebras $B_{D[p^\infty]}$ are fields. But $B_{D[p^\infty]} = K\langle {}^h B_{D[p^\infty]}{}^\times\rangle$ and ${}^h B_{D[p^\infty]}{}^\times \subseteq {}^h B^\times = U$ are essential extensions of $K^\times$ such that $[{}^h B_{D[p^\infty]}{}^\times : K^\times]$ is a power of p and the results follow from Lemma 2.4, Lemma 2.5 and Lemma 2.7. □

If the factor group $U/K^\times$ of the extension $K^\times \hookrightarrow U$ is a finite cyclic group Theorem 2.9 is the well known Theorem of Capelli (for the separable case).

Obviously, if $K\langle U\rangle$ is a field then $K\langle U\rangle$ is a Galois extension of K if and only if the grading group $D = U/K^\times$ has the following property: if D contains an element of order n_0 then $K\langle U\rangle$ contains a root of unity of order n_0. (Note that $K\langle U\rangle$ is by our general assumption always separable.)

3. Applications and Examples

In this section we prove some consequences of the results of section 2. First of all we mention the following slight generalisation of the theorems of Kneser and Schinzel in [6] and [8, Theorem 1], see also [1, Theorem 2.2.1 and Theorem 11.1.5],[10, Theorem 1.12] and [7, §93, Exercise 14].

Theorem 3.1. *Let $L|K$ be a field extension with $(L^\times/K^\times)[\ell^\infty] = 1$, i.e. ${L^\times}^\ell \cap K^\times = {K^\times}^\ell$, if $\operatorname{char} K = \ell > 0$, and let $U \supseteq K^\times$ be a subgroup of $L^\times$. Furthermore, let x_i, $i \in I$, be a full system of representatives for the elements of $U/K^\times$. Then $E := \sum_{i\in I} Kx_i$ is a K-subalgebra of L and the following conditions are equivalent:*

(1) *E is a field and the x_i, $i \in I$, are linearly independent over K.*

(2) *$K^\times \hookrightarrow U$ is an essential extension of groups and $1 + i \notin U$ if U contains a root of unity i of order 4 not in $K^\times$.*

If these conditions hold E is a separable algebraic field extension of degree $[E : K] = [U : K^\times]$.

Proof. First of all, the extension $K^\times \subseteq U$ fulfills by assumption the condition $(U/K^\times)[\ell^\infty] = 1$ if $\operatorname{char} K = \ell > 0$. Consider the universal algebra $K\langle U\rangle$ and the canonical K-algebra homomorphism $\psi : K\langle U\rangle \to E$ induced by the inclusion $U \to E^\times$. Condition (1) is equivalent with the condition that $K\langle U\rangle$ is a field. Now apply Theorem 2.9. □

Note that in 3.1 the algebra E is a priori a field if the extension $L|K$ is algebraic.

The following definitions and results are inspired by the book [1] of T. Albu and the article [4] of C. Greither and D. K. Harrison. We also mention the work [10] of D. Stefan where one can find similar graded formulations for finite field extensions.

Definition 3.2. A group extension $K^\times \hookrightarrow U$ with factor group $D = U/K^\times$ and universal unitarily D-graded K-algebra $L := K\langle U\rangle$ is called *co-Galois* if the following conditions are fulfilled:

(1) L is a field and $D[\ell^\infty] = 0$ if $\operatorname{char} K = \ell > 0$.

(2) Every intermediate field $K \subseteq E \subseteq L$ is graded, i.e. $E = L_{D'}$ for some subgroup $D' \subseteq D$.

We call a field extension $L|K$ *co-Galois* if there exists a co-Galois group extension $K^\times \hookrightarrow U$ such that $L \cong K\langle U\rangle$. In this case the extension $K^\times \subseteq U$ is uniquely determined as we will see after the proof of Theorem 3.3, therefore we drop U from our notation. The condition $D[\ell^\infty] = 0$ if $\operatorname{char} K = \ell > 0$ implies that a co-Galois extension is a separable (algebraic) field extension. A co-Galois extension $L|K$ is our graded equivalent of a *U-Cogalois* extension introduced in [1, Definition 4.3.3 and Definition 12.1.1].

For a co-Galois extension $K \subseteq L = K\langle U\rangle$ and a subgroup $D' \subseteq D = U/K^\times$ the subfield $L_{D'}$ is co-Galois over K and L is co-Galois over $L_{D'}$ (with respect to the induced D/D'-grading). We have maps $D' \mapsto L_{D'}$ and $E \mapsto D_E$ between the set of subgroups of D and the set of intermediate fields of $L|K$ which are inverse to each other. Hence, they are (lattice) isomorphisms.

If $L = K\langle U\rangle$ is co-Galois and $x = \sum_{d\in D} x_d$ is an element in L then $K[x] = K[x_d : d \in D] = L_{\langle \operatorname{supp} x\rangle}$ where $\langle \operatorname{supp} x\rangle$ is the subgroup of D generated by the *support* $\operatorname{supp} x := \{d \in D : x_d \neq 0\}$ of x. In particular, $[K[x] : K] = |\langle \operatorname{supp} x\rangle|$ and $K[x] = L$ if and only if $\langle \operatorname{supp} x\rangle = D$ (cf. also [1, Theorem 8.1.2 and Proposition 10.1.12] and [10, Proposition 2.6]). *If L is co-Galois then any $x \in L^\times$ with $x^2 \in K^\times$ is homogeneous. Proof:* If

$x \notin K$ then $[K[x] : K] = 2$, $\operatorname{char} K \neq 2$ and $x = x_0 + x_d$ with $2d = 0$, $x^2 = x_0^2 + x_d^2 + 2x_0x_d = x_0^2 + x_d^2$ implies $x_0x_d = 0$, i.e. $x_0 = 0$. Examples of co-Galois extensions are the Kummer extensions, cf. Proposition 2.2.

For the following characterisation of co-Galois extensions compare also [1, Theorem 4.3.2] and [10, Theorem 2.5] for the case of an finite extension and [1, Theorem 12.1.4] for the infinite case.

Theorem 3.3. *The group extension $K^\times \hookrightarrow U$ with factor group $D = U/K^\times$ and universal unitarily D-graded K-algebra $L := K\langle U\rangle$ is co-Galois if and only if the following conditions are fulfilled:*

(1) *D is a torsion group with $D[\ell^\infty] = 0$ if $\operatorname{char} K = \ell > 0$.*

(2) *For all primes p with $D[p^\infty] \neq 0$ every element of order p in $L^\times$ belongs to $K^\times$.*

(3) *If D and $K\langle U\rangle^\times$ contain elements of order 4 then $K^\times$ contains an element of order 4.*

Proof. Let $L = K\langle U\rangle$ be co-Galois. Then $K^\times \hookrightarrow U$ is essential by 2.3 and, in particular, $D = U/K^\times$ is a torsion group.

Assume now that D contains an element of prime order p and let $x \in U$ represent such an element. Furthermore, let $\zeta_p \neq 1$ a p-th root of unity in L. Then $\prod_{k=0}^{p-1}(X - \zeta_p^k x) = X^p - x^p$ is the minimal polynomial over K for all the elements $\zeta_p^k x$, $k = 0, \dots, p-1$. The subfield $K[x, \zeta_p]$ is of degree pm with $m < p$ and hence contains only one subfield of degree p over K since all subfields are graded. It follows $K[x] = K[\zeta_p x]$ and $\zeta_p = (\zeta_p x)/x \in K[x]$, i.e. $\zeta_p \in K$.

Let $i \in L^\times$ be a root of unity of order 4 and let $x \in U$ be an element representing an element of order 4 in D. Then i is homogeneous and $\prod_{k=0}^{3}(X - i^k x) = X^4 - x^4$ is the minimal polynomial over K for all the elements $i^k x$, $k = 0, \dots, 3$. Furthermore, $((1+i)x)^4 = (x+ix)^4 = -4x^4 \in K^\times$, hence $[K[(1+i)x] : K] \leq 4$. If $i \notin K^\times$ then ix is homogeneous with $\deg x \neq \deg ix$ and therefore $K[(1+i)x] = K[x, ix] = K[x] = K[ix]$ and $i \in K[x]$, $K[i] = K[x^2]$, i.e. $\deg i = \deg x^2 = 2 \deg x$, which implies $((1+i)x)^2 = 2ix^2 \in K^\times$. This is a contradiction!

To prove that conversely conditions (1),(2),(3) imply that $L = K\langle U\rangle$ is co-Galois over K we can assume that $D = U/K^\times$ is finite.

Conditions (1) and (2) imply that the extension $K^\times \hookrightarrow U$ is essential. Suppose that U contains an element y of order 4 not in $K^\times$, and assume that $x^4 = -4$, $x \in U$. This implies $y^2 = -1 = (x^2/2)^2$, hence $y = \pm x^2/2$ (since $K^\times \hookrightarrow U$ is essential) and $x^2 \notin K^\times$. Therefore, x represents an element of order 4 in D. By assumption (3) this implies that $K^\times$ contains an element i of order 4. Then $(y/i)^2 = 1$ and $y/i = \pm 1$, $y = \pm i \in K^\times$. Contradiction. By Theorem 2.9 L is a field.

Now, let E be an intermediate field, $K \subseteq E \subseteq L = K\langle U\rangle$. We have to show: $E = K\langle U \cap E^\times\rangle$. Consider the group extension $E^\times \hookrightarrow E^\times U$ $(\subseteq L^\times)$ with index $[E^\times U : E^\times] = [U : U \cap E^\times]$. If the universal algebra $E\langle E^\times U\rangle$

is a field then the canonical homomorphism $E\langle E^\times U\rangle \to L = E[E^\times U]$ is an isomorphism which implies $[L : E] = [E^\times U : E^\times] = [U : U \cap E^\times] = [L : K\langle U \cap E^\times\rangle]$ and $E = K\langle U \cap E^\times\rangle$ because of $K\langle U \cap E^\times\rangle \subseteq E$.

So we have to verify that $E^\times \hookrightarrow E^\times U$ fulfills the conditions of Theorem 2.9. The assumption (2) implies that $E^\times \hookrightarrow E^\times U$ is essential. Now suppose that $E^\times U$ contains an element i of order 4 not in $E^\times$ and $x^4 = -4$ with $x \in E^\times U$. The element x represents an element of order 4 in $E^\times U/E^\times \cong U/U \cap E^\times$ because $(x^2/2)^2 = -1 = i^2$ and $x^2 = \pm 2i \notin E^\times$. But then $D = U/K^\times$ contains an element of order 4 and by condition (3) $i \in K$. Contradiction. □

We remark *that for a co-Galois extension $L = K\langle U\rangle$ of K the group $U =^h L^\times$ of homogeneous units is uniquely determined,* cf. also [1, Corollary 4.4.2 and Corollary 10.1.11]. (L may have however unitary gradings which are not co-Galois, cf. Example 2.1.) *Proof:* Let $L = K\langle U'\rangle$ be another co-Galois grading and let $x \in U'$. We have to show $x \in U$. We may assume that the order of x in $U'/K^\times$ is a power of a prime p, i.e that $[K[x] : K] = p^\alpha$, $\alpha \geq 1$, and that $L = K[x]$. If $p \geq 3$ then x represents an element of $(L^\times/K^\times)[p^\infty]$ and belongs therefore to U by Theorem 2.9.

If $p = 2$ then again $x \in U$. This follows from 2.9 if U does not contain an element of order 4 not in $K^\times$. If $i = \sqrt{-1} \in U$, $i \notin K^\times$, then D is an elementary abelian 2-group by condition (3) in Theorem 3.3 and the homogeneous elements $x \in L$ for both gradings are characterised by the condition $x^2 \in K$ (cf. also Proposition 2.2). □

Furthermore, *if $L = K\langle U\rangle$ is a co-Galois extension then $(L^\times/K^\times)[p^\infty] = (U/K^\times)[p^\infty]$ for every prime $p \geq 3$ with $(U/K^\times)[p^\infty] \neq 1$ and the equality $(L^\times/K^\times)[2^\infty] = (U/K^\times)[2^\infty]$ holds in the following cases:* (1) *$U/K^\times$ contains an element of order* 4, (2) *$i(= \sqrt{-1}) \in K^\times$*, (3) *$i \notin L^\times$. In any case the equality $(L^\times/K^\times)[2] = (U/K^\times)[2]$ holds*(compare also with [1, Theorem 4.4.1 and Theorem 12.1.8]). The equality $(L^\times/K^\times)[p^\infty] = (U/K^\times)[p^\infty]$ for a prime number $p \geq 2$ is equivalent to the property that $K\langle \mathrm{T}_p(L^\times/K^\times)\rangle$ is a field, where $\mathrm{T}_p(L^\times|K^\times)$ is by definition the canonical preimage of $(L^\times/K^\times)[p^\infty]$ in $L^\times$ and this is checked with Theorem 2.9 using the characterisation of co-Galois extensions in Theorem 3.3.

Let $\mathrm{T}(L^\times|K^\times) = \{x \in L^\times : x^n \in K^\times \text{ for some } n\} \subseteq L^\times$ denote the canonical preimage in $L^\times$ of the torsion subgroup $\mathrm{t}(L^\times/K^\times)$ of $L^\times/K^\times$. (In [4] the group $\mathrm{t}(L^\times/K^\times)$ is called the *co-Galois group* of $L|K$.)

Definition 3.4. A field extension $L|K$ is called *absolutely co-Galois* if the canonical K-algebra homomorphism $K\langle \mathrm{T}(L^\times|K^\times)\rangle \to L$ induced by the inclusion $\mathrm{T}(L^\times|K^\times) \hookrightarrow L^\times$ is an isomorphism.

In an equivalent, but different approach finite absolutely co-Galois extensions were treated in [4] and called *cogalois extensions*, see also [1, Definition 12.2.1] for the infinite case. We prefer the term absolutely co-Galois in order to stress that the grading group is the whole torsion group of $L^\times/K^\times$.

If $L|K$ is absolutely co-Galois then L is unitarily $\mathrm{t}(L^\times/K^\times)$-graded and ${}^hL^\times = \mathrm{T}(L^\times|K^\times)$. *The extension is necessarily separable.* For the *proof*, let

$x \in L^\times$, $x^\ell \in K^\times$, $\ell := \operatorname{char} K > 0$. Then $(1+x)^\ell \in K^\times$ which implies $x \in K$ since $1, x, 1+x$ are homogeneous. This means $(L^\times/K^\times)[\ell^\infty] = 1$.

The following characterisation of absolutely co-Galois extensions is a direct consequence of Theorem 2.9. One compares also [4, Theorem 1.5] and [1, Theorem 3.1.7] for finite extensions as well as [1, Theorem 12.2.2] for the infinite case.

Theorem 3.5. *A field extension $L|K$ is absolutely co-Galois if and only if the following conditions are fulfilled:*

(1) *The group $\mathrm{T}(L^\times|K^\times)$ generates L as a K-algebra, the group extension $K^\times \hookrightarrow \mathrm{T}(L^\times|K^\times)$ is essential and $(L^\times/K^\times)[\ell^\infty] = \mathrm{T}_\ell(L^\times|K^\times)/K^\times = 1$, i.e. ${L^\times}^\ell \cap K^\times = {K^\times}^\ell$, if* $\operatorname{char} K = \ell > 0$.

(2) *If $L^\times$ contains a root of unity i of order 4 then i belongs already to $K^\times$.*

For the following two easy corollaries compare also [4, Theorem 1.6.(a)], [1, Proposition 3.2.2.(2) and Theorem 12.2.4.(4)] and [1, Theorem 12.2.3] respectively.

Corollary 3.6. *If $L|K$ is an absolutely co-Galois extension, then for any intermediate field E the extensions $L|E$ and $E|K$ are absolutely co-Galois too.*

Theorem 3.3 implies:

Corollary 3.7. *An absolutely co-Galois extension $L|K$ is co-Galois with respect to the group extension $K^\times \hookrightarrow \mathrm{T}(L^\times|K^\times)$ and with grading group $\mathrm{T}(L^\times|K^\times)/K^\times = \mathrm{t}(L^\times/K^\times)$.*

Co-Galois extensions are not necessarily absolutely co-Galois. Look at $\mathbb{Q}[\zeta_3]|\mathbb{Q}$ or as an extreme case $\mathbb{C}|\mathbb{R}$. A co-Galois extension $L = K\langle U\rangle$ over K is absolutely co-Galois if and only if the following conditions are fulfilled: (1) Any root of unity ζ_q of prime order q in $L^\times$ with $(U/K^\times)[q^\infty] = 1$ belongs already to $K^\times$. (2) If the element i of order 4 belongs to $L^\times$ then $i \in K^\times$. (If $i \notin K^\times$ then $K[i]$ is never absolutely co-Galois.)

Example 3.8. Let K be a field which contains for every prime $p \neq \operatorname{char} K$ a root of unity of order p and a root of unity of order 4 if $\operatorname{char} K \neq 2$. Furthermore, let $\bar{K}_{\mathrm{sep}}$ be the separable algebraic closure of K. Then the group $\mathrm{T}(\bar{K}_{\mathrm{sep}}^\times|K^\times)$ is an essential extension of $K^\times$, indeed $\mathrm{T}(\bar{K}_{\mathrm{sep}}^\times|K^\times) = \mathrm{I}'(K^\times)$ where $\mathrm{I}'(K^\times) \subseteq \mathrm{I}(K^\times)$ is the preimage of $\prod_{p\in\mathbb{P}, p\neq \operatorname{char} K}(\mathrm{I}(K^\times)/K^\times)[p^\infty]$ in the injective hull $\mathrm{I}(K^\times)$ of the group $K^\times$. The equality $\mathrm{I}'(K^\times) = \mathrm{I}(K^\times)$ holds if and only if K is a perfect field.

Since the group extension $K^\times \hookrightarrow \mathrm{T}(\bar{K}_{\mathrm{sep}}^\times|K^\times) = I'(K^\times)$ is co-Galois by Theorem 3.3 the canonical homomorphism $K\langle I'(K^\times)\rangle \to \bar{K}_{\mathrm{sep}}$ is injective and *its image $K[I'(K^\times)]$ is the largest absolutely co-Galois extension of* K, cf. Theorem 3.5. It is also a Galois extension which contains *all* roots of unity, i.e. for any $n \in \mathbb{N}^*$ with $n \neq 0$ in K there is a root of unity of order n in $K[\mathrm{I}'(K^\times)]$.

Furthermore, if K contains *all* roots of unity then this extension coincides with the largest Kummer extension of K which is in this case also the largest abelian extension $\bar{K}_{\mathrm{ab}}$ of K. The Galois group of this extension is the character group $\mathrm{Hom}(\mathrm{I}'(K^\times)/K^\times, K^\times) = \mathrm{Hom}(\mathrm{I}'(K^\times)/K^\times, \mathbb{Q}/\mathbb{Z})$ of $\mathrm{I}'(K^\times)/K^\times = \mathrm{t}(\bar{K}^\times_{\mathrm{sep}}/K^\times)$, cf. Proposition 2.2.

So if we iterate this construction starting with $K_1 := K[\mathrm{I}'(K^\times)]$ instead of $K_0 := K$ we get the Kummer extension $K_2 := K_1[\mathrm{I}'(K_1^\times)]$ of K_1 and altogether a tower of subfields $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$ of $\bar{K}_{\mathrm{sep}}$ such that every extension $K_{j+1}|K_j$, $j \in \mathbb{N}$, is absolutely co-Galois (and Kummer for $j > 0$).

If F is an arbitrary field then take for K_0 the field $K := F[\zeta_p, p \in \mathbb{P}, p \neq \mathrm{char}\, F; i]$, where $\zeta_p \in \bar{F}_{\mathrm{sep}} (= \bar{K}_{\mathrm{sep}})$ is a root of unity of order p (and $i \in \bar{K}_{\mathrm{sep}}$ of order 4 if $\mathrm{char}\, F \neq 2$). If $\mathrm{char}\, F = 0$ then $\bigcup_{j\geq 0} K_j = \bar{F}_{\mathrm{solv}}$ is the union of all Galois extensions of F in $\bar{F}_{\mathrm{sep}} = \bar{F}$ with solvable Galois group.

Example 3.9. Let K be an *ordered* field and let $\bar{K}_{\mathrm{real}}$ be the real closure of K. Then the group $\mathrm{T}(\bar{K}^\times_{\mathrm{real}}|K^\times)$ is an essential extension of $K^\times$ since ± 1 are the only roots of unity in $\bar{K}^\times_{\mathrm{real}}$, indeed $\mathrm{T}(\bar{K}^\times_{\mathrm{real}}|K^\times) = \{\pm 1\}\,\mathrm{I}(K^\times_+)$, where $\mathrm{T}(\bar{K}^\times_{\mathrm{real},+}|K^\times_+) = \mathrm{I}(K^\times_+) \subseteq \bar{K}^\times_{\mathrm{real},+}$ is the injective hull of the group of positive elements in K.

Since the group extension $K^\times \hookrightarrow \mathrm{T}(\bar{K}^\times_{\mathrm{real}}|K^\times)$ is co-Galois by Theorem 3.3 *the canonical homomorphism* $K\langle\{\pm 1\}\,\mathrm{I}(K^\times_+)\rangle \to \bar{K}_{\mathrm{real}}$ *is injective* and *its image* $K[\mathrm{I}(K^\times_+)]$ *is the largest co-Galois extension of* K *in* $\bar{K}_{\mathrm{real}}$. *It is even absolutely co-Galois*, cf. Theorem 3.5.

In case that $K = \mathbb{Q}$ or, more generally, that K is a real algebraic number field the injectivity of the canonical map $K\langle\{\pm 1\}\,\mathrm{I}(K^\times_+)\rangle \to \bar{K}_{\mathrm{real}} \subseteq \mathbb{R}$ is a classical result of Besicovitch [2] and Siegel [9].

That $\mathbb{Q} \subseteq \mathbb{Q}[\mathrm{I}(\mathbb{Q}^\times_+)]$ is a co-Galois extension can be expressed in the following way: If $(\nu_{1\sigma}, \ldots, \nu_{r\sigma}) \in \mathbb{Q}^r$, $\sigma = 1, \ldots, s$, are r-tuples which represent different elements in $(\mathbb{Q}/\mathbb{Z})^r$ and if $p_1, \ldots, p_r$ are different prime numbers then the degree of every element

$$x = \sum\nolimits_{\sigma=1}^{s} a_\sigma p_1^{\nu_{1\sigma}} \cdots p_r^{\nu_{r\sigma}}$$

with $a_1, \ldots, a_s \in \mathbb{Q}^\times$ is $|d|$ where $1/d$ is the greatest common divisor of *all* the minors (including 1) of the $r \times s$-matrix $(\nu_{\rho\sigma})_{1\leq\rho\leq r, 1\leq\sigma\leq s}$; for instance, $x := 2^{1/2}3^{1/4} + 2^{1/3}3^{1/2}$ has degree 12 over $\mathbb{Q}$ and $\mathbb{Q}[x] = \mathbb{Q}[2^{1/2}3^{1/4}, 2^{1/3}3^{1/2}]$ $(= \mathbb{Q}[2^{1/6}3^{1/4}])$, cf. [1], Example 9.2.9.

In a similar way, the finite subextensions of $K[\mathrm{I}(K^\times_+)]$ can be described for a *finite* real number field K: The multiplicative group $K^\times_+$ of the positive numbers in K is free. (For any finite number field K the group $K^\times/\mu(K)$ ($\mu(K) :=$ group of roots of unity in K) is free.) If a basis π_i, $i \in I$, of $K^\times_+$ is given (and such a basis can be constructed in principle) one has completely analogous results for K instead of $\mathbb{Q}$, replacing the primes $p \in \mathbb{P}$ by the π_i, $i \in I$. (Even the assumption that K is a real field is not essential. One replaces $K^\times_+$ by $K^\times/\mu(K)$.)

Iterating the construction $K\langle\{\pm 1\}\,\mathrm{I}(K^\times_+)\rangle$ from K, we get a tower of fields $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq \bar{K}_{\mathrm{real}}$ with $K_{j+1} = K_j[\mathrm{I}(K^\times_{j,+})] = K_j\langle\{\pm 1\}\,\mathrm{I}(K^\times_{j,+})\rangle$ for an ordered field K. It is an interesting task to determine for a given $x \in \bigcup_j K_j$ the smallest $j \in \mathbb{N}$ with $x \in K_j$.

Example 3.10. Any essential group extension $\mathbb{Q}^\times \hookrightarrow U$ can be embedded into the injective hull $\mathrm{I}(\mathbb{Q}^\times) = \mathrm{I}(\{\pm 1\}) \times \mathrm{I}(\mathbb{Q}^\times_+)$ and hence the universal algebra $\mathbb{Q}\langle U\rangle$

into $\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$. We use the canonical identification $\mathrm{I}(\mathbb{Q}^\times) = \mathrm{I}(\{\pm 1\}) \times \mathrm{I}(\mathbb{Q}^\times_+) = S^1[2^\infty] \times \mathrm{T}(\mathbb{R}^\times_+|\mathbb{Q}^\times_+) \subseteq S^1 \times \mathbb{R}^\times_+ = \mathbb{C}^\times$, $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. The group $\mathrm{I}(\mathbb{Q}^\times_+) = \mathrm{T}(\mathbb{R}^\times_+|\mathbb{Q}^\times_+)$ is torsion-free and divisible with the primes $p \in \mathbb{P}$ as canonical $\mathbb{Q}$-basis and was studied in the previous example.

The universal algebra $\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$ is *not* a field because of $i \in S^1[2^\infty] \subseteq \mathrm{I}(\mathbb{Q}^\times)$, $i \notin \mathbb{Q}^\times$ and $(1+i) = \zeta_8\sqrt{2} \in \mathrm{I}(\mathbb{Q}^\times)$, $(1+i)^4 = -4$, cf. Theorem 2.9.

To understand $\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$ we compare this algebra with the universal $\mathbb{Q}[i]$-algebra $\mathbb{Q}[i]\langle \mathrm{I}(\mathbb{Q}[i]^\times)\rangle$ which is by Theorem 2.9 a field.

Also $\mathrm{I}(\mathbb{Q}[i]^\times)$ can be identified with a subgroup of $\mathbb{C}^\times$ which extends the identification of $\mathrm{I}(\mathbb{Q}^\times)$ as a subgroup of $\mathbb{C}^\times$ from above. We have to choose $\mathrm{t}(\mathrm{I}(\mathbb{Q}[i]^\times)) = S^1[2^\infty]$ and take for the primes $q \in \mathbb{Z}[i]$ with $-\pi/4 < \arg q < \pi/4$ the element $\exp(\alpha \ln q)$ as q^α, $\alpha \in \mathbb{Q}$, and identify $p^\alpha \in \mathrm{I}(\mathbb{Q}^\times)$, $\alpha \in \mathbb{Q}$, $p \geq 3$ prim in $\mathbb{Z}$, in the natural way with $p^\alpha \in \mathrm{I}(\mathbb{Q}[i]^\times)$. For the prime $1+i \in \mathbb{Z}[i]$ and for $2 = (-i)(1+i)^2 \in \mathbb{Z}$ we proceed as follows: $(1+i)^\alpha$, $\alpha \in \mathbb{Q}$, we will identify with $\exp(2\pi i(\alpha/8)_2)2^{\alpha/2}$, where r_2 for $r \in \mathbb{Q}$ denotes the 2-component of $[r] \in \mathbb{Q}/\mathbb{Z} = \bigoplus_{p\in\mathbb{P}}(\mathbb{Q}/\mathbb{Z})[p^\infty] = \bigoplus_{p\in\mathbb{P}}(\mathbb{Z}_{(p^k,\, k\in\mathbb{N})}/\mathbb{Z})$. Then $1+i$ will be identified with $\exp(2\pi i/8)\sqrt{2} = 1+i$ (and hence $(1+i)^n$ with $(1+i)^n$ for all $n \in \mathbb{Z}$). The element $2^\alpha \in \mathrm{I}(\mathbb{Q}^\times)$, $\alpha \in \mathbb{Q}$, has in $\mathrm{I}(\mathbb{Q}[i]^\times)$ the representation $2^\alpha = \exp(-2\pi i(\alpha/4)_2)(1+i)^{2\alpha}$.

The kernel of the universal homomorphism $\varphi : \mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle \to \mathbb{Q}[i]\langle \mathrm{I}(\mathbb{Q}[i]^\times)\rangle$ *is the principal ideal generated by* $f := x^2 - 2x + 2 = (2i+2) - \zeta_8\sqrt{2}$, *with* $x := \zeta_8\sqrt{2} \in \mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle = \mathbb{Q}[i]\langle \mathbb{Q}[i]^\times * \mathrm{I}(\mathbb{Q}^\times)\rangle$ *and* $x^4 = -4$ (where $*$ denotes the multiplication in $\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$ which has to be distinguished from the multiplication in $\mathbb{Q}[\mathrm{I}(\mathbb{Q}^\times)] \subseteq \mathbb{C}$). This assertion follows from the fact that fx_j, $j \in J$, generate $\ker\varphi$ as a $\mathbb{Q}[i]$-vector space if x_j, $j \in J$, represent the elements of the factor group $\mathbb{Q}[i]^\times * \mathrm{I}(\mathbb{Q}^\times)/\mathbb{Q}[i]^\times$. *Therefore* $\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle / f\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$ *is isomorphic to the subfield* $\mathbb{Q}[\mathrm{I}(\mathbb{Q}^\times)] \subseteq \mathbb{C}$. The principal ideal (f) can also be generated by the idempotent element $e := (x+2)f/8$. If we use the automorphism of $\mathrm{I}(\mathbb{Q}^\times)$ induced by taking the 5-th power on the component $S^1[2^\infty]$ of $\mathrm{I}(\mathbb{Q}^\times)$ and the identity on the other components we get an automorphism $\Psi : \mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle \to \mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$. The kernel of the homomorphism $\varphi \circ \Psi^{-1} : \mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle \to \mathbb{Q}[i]\langle \mathrm{I}(\mathbb{Q}[i]^\times)\rangle$ is generated by $\Psi(e) = (-x+2)\Psi(f)/8 = 1 - e$.

It follows that $\mathbb{Q}\langle \mathrm{I}(\mathbb{Q}^\times)\rangle$ *is the product of two fields which are both isomorphic to* $\mathbb{Q}[\mathrm{I}(\mathbb{Q}^\times)] \subseteq \mathbb{C}$. For any essential group extension U of $\mathbb{Q}^\times$ we have inclusions $\mathbb{Q}^\times \subseteq U \subseteq \mathrm{I}(\mathbb{Q}^\times)$. Hence: *If* $\mathbb{Q}\langle U\rangle$ *is not a field, i.e. if* $-4 \in U^4$ *then* $\mathbb{Q}\langle U\rangle$ *decomposes into two fields.* But, these fields are not necessarily isomorphic. Perhaps the simplest example is $\mathbb{Q}\langle U\rangle := \mathbb{Q}[X]/(X^{16}+4) \cong (\mathbb{Q}[X]/(X^8 - 2X^4 + 2)) \times (\mathbb{Q}[X]/(X^8 + 2X^4 + 2)) = K_1 \times K_2$, $K_1 \ncong K_2$. To prove this, one computes for instance the Galois group $\mathrm{G}(L|K)$ of the splitting field L of $X^{16}+4$ over $\mathbb{Q}$ and considers K_1 and K_2 as subfields of L. The Galois group is isomorphic to the semidirect product $(\mathbb{Z}_4 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_2$ where $\mathbb{Z}_2$ is generated by the complex conjugation κ which operates on $\mathbb{Z}_4 \times \mathbb{Z}_4$ as the matrix

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

The two factors of the product group $\mathbb{Z}_4 \times \mathbb{Z}_4$ (which are not conjugated in $(\mathbb{Z}_4 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_2$) are the subgroups belonging to K_1 and K_2.

4. Unitarily graded Galois extensions

We consider finite Galois field extensions $L|K$. (We leave the easy generalisations to infinite Galois extensions to the reader. One simply uses the fact that in the graded case $L = K\langle U\rangle = \varinjlim K\langle U'\rangle$ where U' runs through the subgroups $U' \subseteq U = {}^hL^\times$ with $K^\times \subseteq U'$ and $[U' : K^\times] < \infty$.) Let us start with the case where the Galois group is cyclic. If L has a unitary grading over K then the grading group D is necessarily also cyclic. To prove this, observe that any subgroup $D' \subseteq D$ defines the graded subfield $L_{D'}$. Therefore, for any divisor d' of $|D| = \operatorname{ord} D$, there exists at most one subgroup of D of order d'. But this condition characterises the finite cyclic groups in the class of all finite (not necessarily abelian) groups D (indeed, it suffices to consider prime powers d' dividing $|D|$). Moreover, if the cyclic extension $L|K$ has a grading then this grading is even co-Galois and hence essentially unique (in the sense that the group of homogeneous units is unique). Conversely, if a Galois extension has a co-Galois grading with cyclic grading group then the Galois group is also cyclic. More generally, the following is true.

Lemma 4.1. *Let $L|K$ be a finite Galois field extension with a D-co-Galois grading. Then* $\exp(D) = \exp(\mathrm{G}(L|K))$ *and there is an element* $\sigma \in \mathrm{G}(L|K)$ *with* $\operatorname{ord}\sigma = \exp(\mathrm{G}(L|K))$.

Proof. Let $\sigma \in G := \mathrm{G}(L|K)$. Then L is graded over the σ-invariant field $L^\sigma = L_{D'}$ with grading group D/D' for some subgroup $D' \subseteq D$. The extension $L|L^\sigma$ is cyclic of degree $\operatorname{ord}\sigma$. It follows that D/D' is also cyclic of the same order. This proves $\exp(G)|\exp(D)$. For the converse let $D' \subseteq D$ be a subgroup with cyclic quotient D/D' of order $\exp(D)$. Then the Galois extension $L|L_{D'}$ has a D/D'-co-Galois grading. By the remark above, $\mathrm{G}(L|L_{D'}) \subseteq \mathrm{G}(L|K) = G$ is cyclic of order $|D/D'| = \exp(D)$. □

If the (finite) Galois extensions $L_\sigma|K$, $\sigma = 1, \dots, s$, have a co-Galois grading and if $L := L_1 \otimes_K \cdots \otimes_K L_s$ is a field (i.e. if the L_σ are linearly disjoint over K), then the grading of L derived from the gradings of the factors is also co-Galois. This follows immediately from the fact that for this grading of L the conditions of Theorem 3.3 are fulfilled since these conditions are fulfilled for the factors. Note that a D-graded Galois extension contains a root of unity of order m if D contains an element of order m. (In general, the product $L_1 \otimes_K L_2$ of co-Galois extensions is not co-Galois even if L_1, L_2 are linearly disjoint. For example, $\mathbb{Q}[\sqrt[3]{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\zeta_3]$ has no co-Galois grading at all.)

Let us now assume that the extension $L|K$ is abelian with Galois group $G := \mathrm{G}(L|K)$ and that it has a co-Galois grading with $U = {}^hL^\times$ as group of homogeneous units and grading group $D \cong U/K^\times$. Then we can prove a little bit more. If $D = D_1 \times \cdots \times D_r$ is a decomposition of D into cyclic factors D_ρ, $\rho = 1, \dots, r$, then the subfields L_{D_ρ} are also co-Galois and Galois. Hence the Galois group $G_\rho := \mathrm{G}(L_{D_\rho}|K)$ is cyclic too and $G_\rho \cong D_\rho$. It follows the (non canonical) isomorphism $G = \mathrm{G}(L_{D_1} \otimes_K \cdots \otimes_K L_{D_r}|K) =$

$G_1 \times \cdots \times G_r \cong D_1 \times \cdots \times D_r = D$ (compare also [10, Theorem 2.9]). Conversely, if the grading group D of an arbitrary unitary grading of an (abelian) extension $L|K$ is isomorphic to the Galois group G, then the grading is co-Galois because the mapping $D' \mapsto \mathrm{G}(L|L_{D'})$ is an injective and hence bijective map from the set of subgroups $D' \subseteq D$ into the set of subgroups of G.

A (not necessarily abelian) Galois extension L of K which has a co-Galois grading contains necessarily a root of unity of order n where $n := \exp(D) = \exp(\mathrm{G}(L|K))$. The base field K contains necessarily a root of unity of order p for every prime divisor p of n and moreover a root of unity of order 4 if $4|n$, cf. Theorem 3.3. Altogether, K contains a root of unity of order $\mathrm{er}(n)$ where $\mathrm{er}(n)$ is the *extended reduction* of n defined by

$$\mathrm{er}(n) := \begin{cases} \mathrm{r}(n), & \text{if } 4\not|n, \\ 2\,\mathrm{r}(n), & \text{if } 4|n. \end{cases}$$

Here the *reduction* $\mathrm{r}(n)$ of n is the product of the prime factors of n.

The elements of the Galois group G of $L|K$ are explicitly given by the formula

$$\sigma_\chi\left(\sum\nolimits_d x_d\right) = \sum\nolimits_d \chi(d)x_d,$$

where the index χ runs through the character group $\check{D} = \mathrm{Hom}(D, L^\times) = \mathrm{Hom}(D, \mu_n(L))$, $n = \exp(D)$. *It follows that $\mu_n(L) \subseteq U =^h L^\times$ since $\sigma_\chi(U) = U$ for all $\chi \in \check{D}$ (the co-Galois grading is essentially unique!) and hence $\chi(d) = \sigma_\chi(x_d)/x_d \in U$ for all $\chi \in \check{D}$ and all homogeneous units x_d of degree d, $d \in D$.*

The group $U = {}^hL^\times$ can be described in the following way using only the Galois group G: *It is*

$$U/\mu_n(L) = (L^\times/\mu_n(L))^G$$

(where $n = \exp(G)$ and the operation of G on $L^\times/\mu_n(L)$ is induced by the Galois operation). We have only to show the inclusion $U' \subseteq U$, where $U' \subseteq L^\times$ is defined by the equation $U'/\mu_n(L) = (L^\times/\mu_n(L))^G$. From the exact sequence of group cohomology

$$1 \to \mu_n(L)^G = \mu_n(K) \to (L^\times)^G = K^\times \to (L^\times/\mu_n(L))^G = U'/\mu_n(L) \to \mathrm{H}^1(G, \mu_n(L))$$

we derive the exact sequence

$$1 \longrightarrow \mu_n(L)/\mu_n(K) \longrightarrow U'/K^\times \longrightarrow \mathrm{H}^1(G, \mu_n(L)).$$

It follows that $U'/K^\times$is a finite group since $\mathrm{H}^1(G, \mu_n(L))$ is finite. Moreover, the exponent of $\mathrm{H}^1(G, \mu_n(L))$ divides $n = \exp(G) = |\mu_n(L)|$.

We show that the universal algebra $K\langle U'\rangle$ is a field and use Theorem 2.9 to do this. If p is a prime divisor of $|U'/K^\times|$ then p divides $n = |\mu_n(L)|$ hence $\mathrm{er}(n)$, and K contains a root of unity of order p. This proves that $K^\times \hookrightarrow U'$ is essential. If U' contains an element i of order 4 but $i \notin K^\times$

then $4 \nmid n$ (because $|\mu_{\mathrm{er}(n)}(K)| = \mathrm{er}(n)$ and hence $|\mu_n(L)/\mu_n(K)|$ is odd and $\mathrm{H}^1(G, \mu_n(L))$ does not contain an element of order 4. Then, by the exact sequence above, $U'/K^\times$ contains no element of order 4. It follows $-4 \notin U'^4$. The canonical homomorphism $K\langle U'\rangle \to L$ which extends the isomorphism $K\langle U\rangle \overset{\sim}{\to} K[U] = L$ is injective. This yields $U = U'$.

We notice:

Lemma 4.2. *Let $L|K$ be a finite Galois field extension with Galois group G and $n := \exp(G)$. If $|\mu_n(L)| = n$, $|\mu_{\mathrm{er}(n)}(K)| = \mathrm{er}(n)$ and $U' \subseteq L^\times$ is the subgroup with $\mu_n(L) \subseteq U'$ and $U'/\mu_n(L) = (L^\times/\mu_n(L))^G$ then the universal algebra $K\langle U'\rangle$ is a field isomorphic to $K[U'] \subseteq L$. The canonical sequence*

$$1 \longrightarrow \mu_n(L)/\mu_n(K) \longrightarrow U'/K^\times \longrightarrow \mathrm{H}^1(G, \mu_n(L)) \longrightarrow 1$$

is exact and $K\langle U'\rangle \cong K[U']$ is a co-Galois and Galois extension of K. Moreover, $K[U'] \subseteq L$ is the largest Galois subextension of L which is co-Galois.

Proof. The exact sequence follows from the exact sequence $1 \to \mu_n(L) \to L^\times \to L^\times/\mu_n(L) \to 1$ and $\mathrm{H}^1(G, L^\times) = 1$ (Noether's Theorem). The co-Galois property follows from Theorem 3.3. The extension $K[U']$ is Galois since U' is G-invariant. □

In general, the co-Galois extension $K\langle U'\rangle \cong K[U'] \subseteq L$ of Lemma 4.2 is a proper subfield of L. It coincides with L if and only if $|U'/K^\times| = |G|$ or equivalently

$$|\,\mathrm{H}^1(G, \mu_n(L))| = |\mu_n(K)|\,|G|/n.$$

This proves

Theorem 4.3. *Let $L|K$ be a finite Galois field extension with Galois group G and $n := \exp(G)$. L has a co-Galois grading over K if and only if the following conditions are satisfied:*

(1) *$|\mu_n(L)| = n$ and $|\mu_{\mathrm{er}(n)}(K)| = \mathrm{er}(n)$.*

(2) *$|\,\mathrm{H}^1(G, \mu_n(L))| = |\mu_n(K)|\,|G|/n$.*

In the cyclic case condition (1) in 4.3 is sufficient:

Theorem 4.4. *Let $L|K$ be a finite cyclic field extension of degree n. Then L has a unitary grading (which is necessarily a co-Galois grading) if and only if $|\mu_n(L)| = n$ and $|\mu_{\mathrm{er}(n)}(K)| = \mathrm{er}(n)$.*

Proof. Let the conditions on the roots of unity be satisfied. We have to prove that condition (2) of Theorem 4.3 is also satisfied, which means $|\,\mathrm{H}^1(\mathrm{G}(L|K), \mu_n(L))| = |\mu_n(K)|$. Let σ be a generator of the Galois group $G := \mathrm{G}(L|K)$. Then the cohomology group $\mathrm{H}^1(G, \mu_n(L))$ is the homology of the complex

$$\mu_n(L) \xrightarrow{\sigma/\,\mathrm{id}} \mu_n(L) \xrightarrow{\mathrm{N}} \mu_n(L)$$

of finite groups where N is the norm $x \mapsto \prod_{j=0}^{n-1} \sigma^j x$. It follows from the index satz

$$|\,\mathrm{H}^1(G, \mu_n(L))| = |\ker \sigma / \operatorname{id}|\,|\operatorname{coker} \mathrm{N}\,|/|\mu_n(L)| = |\mu_n(K)|\,|\operatorname{coker} \mathrm{N}\,|/n.$$

It remains to show: $|\operatorname{coker} \mathrm{N}\,| = n$, i.e. $\mu_n(L)$ belongs to the norm-1-group of $L|K$. But this is verified by the following (probably well-known) lemma. □

Lemma 4.5. *Let $L|K$ be a finite field extension of degree n. Then $\mu_n(L)$ is contained in the norm-1-group of $L|K$.*

Proof. It is sufficient to show: If $\zeta \in L$ is a root of unity of prime power order $p^\alpha > 1$ and if p^α divides n, then $\mathrm{N}_K^L(\zeta) = 1$. Consider the subfield $K[\zeta]$ and let $m := [K[\zeta] : K]$. Then $m|n$ and $\mathrm{N}_K^L(\zeta) = \mathrm{N}_K^{K[\zeta]}(\mathrm{N}_{K[\zeta]}^L(\zeta)) = \mathrm{N}_K^{K[\zeta]}(\zeta^{n/m})$ and $\zeta^{n/m} \in \mu_m(K[\zeta])$. Therefore, we may assume additionally $L = K[\zeta]$. $K[\zeta]|K$ is a Galois extension. Its Galois group is a subgroup of the automorphism group $\operatorname{Aut}(\langle\zeta\rangle) = (\mathbb{Z}/\mathbb{Z}p^\alpha)^\times$ and its order m divides $p^{\alpha-1}(p-1)$, i.e. $m = p^\beta t$, $\beta < \alpha$, $t|(p-1)$.

It is enough to prove $\mathrm{N}(\zeta)^{p^{\alpha-\beta}} := \mathrm{N}_{K[\zeta^{p^{\alpha-1}}]}^{K[\zeta]}(\zeta)^{p^{\alpha-\beta}} = 1$. $K[\zeta]|K[\zeta^{p^{\alpha-1}}]$ is a Galois extension of degree p^β and its Galois group G is a subgroup of $1 + \mathbb{Z}p/\mathbb{Z}p^\alpha \subseteq (\mathbb{Z}/\mathbb{Z}p^\alpha)^\times$.

First let $p \geq 3$. Then $G = 1 + \mathfrak{a}$, $\mathfrak{a} := \mathbb{Z}p^{\alpha-\beta}/\mathbb{Z}p^\alpha$ and $\mathrm{N}(\zeta)^{p^{\alpha-\beta}} = \left(\prod_{\sigma\in G} \sigma\zeta\right)^{p^{\alpha-\beta}} = \zeta^{p^{\alpha-\beta}S}$, $S := \sum_{j\in\mathfrak{a}}(1+j) = p^\beta + \sum_{j\in\mathfrak{a}} j = p^\beta$ since $\sum_{j\in\mathfrak{a}} j = 0$, hence $\mathrm{N}(\zeta)^{p^{\alpha-\beta}} = \zeta^{p^{\alpha-\beta}p^\beta} = 1$.

Now let $p = 2$ and $\alpha \geq 2$. Then $1 + \mathbb{Z}2/\mathbb{Z}2^\alpha$ is the product of the cyclic subgroups $\{\pm 1\}$ and $1 + \mathbb{Z}4/\mathbb{Z}2^\alpha$. The subgroups of order 2^β are $1 + \mathfrak{a}$, $\mathfrak{a} := \mathbb{Z}2^{\alpha-\beta}/\mathbb{Z}2^\alpha$ (if $\beta \leq \alpha - 2$) and the groups $(1+\alpha) \uplus -(1+\mathfrak{a})(1+x)$ with $\mathfrak{a} := \mathbb{Z}2^{\alpha-\beta+1}/\mathbb{Z}2^\alpha$ and a fixed $x \in \mathbb{Z}4/\mathbb{Z}2^\alpha$, $(1+x)^2 - 1 = x(2+x) \in \mathfrak{a}$.

In the first case $\mathrm{N}(\zeta)^{2^{\alpha-\beta}} = \zeta^{2^{\alpha-\beta}S}$ with $S := \sum_{j\in\mathfrak{a}}(1+j) = 2^\beta + \sum_{j\in\mathfrak{a}} j = 2^\beta + 2^{\alpha-1}$ if $\beta > 0$ (and $S = 1$ if $\beta = 0$), hence $\mathrm{N}(\zeta)^{2^{\alpha-\beta}} = 1$. In the second case $\mathrm{N}(\zeta)^{2^{\alpha-\beta}} = \zeta^{2^{\alpha-\beta}S}$ with $S := -(\sum_{j\in\mathfrak{a}} j)x - 2^{\beta-1}x$, hence $\zeta^{2^{\alpha-\beta}S} = \zeta^{-2^{\alpha-1}x} = 1$. □

In general, condition (1) in Theorem 4.3 is not sufficient for the existence of a co-Galois grading of $L|K$, even in the abelian case. For instance, the Galois extension $\mathbb{Q}[\sqrt{-3}, \sqrt{-19}] \subseteq \mathbb{Q}[\zeta_{3^2\cdot 19}]$ with Galois group $\mathbb{Z}_3 \times \mathbb{Z}_9$ has no co-Galois grading but $\zeta_9 \in \mathbb{Q}[\zeta_{3^2\cdot 19}]$ and $\zeta_3 \in \mathbb{Q}[\sqrt{-3}, \sqrt{-19}]$. – If the Galois group G of $L|K$ is abelian and contains a subgroup isomorphic to $\mathbb{Z}_n \times \mathbb{Z}_n$, $n = \exp(G)$, then $L|K$ has a co-Galois grading (if and) only if $L|K$ is a Kummer extension, i.e. $|\mu_n(K)| = n$.– Also, if $|\mu_n(K)| = n$ and $L|K$ has a co-Galois grading then G is necessarily abelian, hence $L|K$ is a Kummer extension. It follows, quite generally, that for a finite Galois and co-Galois extension $L|K$ with Galois group G the co-Galois extension $L|K[\zeta_n]$ $(n = \exp(G))$ is a Kummer extension. Since an abelian extension $L|K$ has a co-Galois grading if and only if every cyclic subextension $L'|K$,

$L' \subseteq L$, has such a grading Theorem 4.4 is useful also in this more general setting.

With respect to Lemma 4.5 the group $\mu_n(K) = \mathrm{H}^0(G, \mu_n(L))$ can also be interpreted as the modified cohomology group $\hat{\mathrm{H}}^0(G, \mu_n(L))$ (in the sense of Tate). Since $\hat{\mathrm{H}}^1(G, \mu_n(L)) = \mathrm{H}^1(G, \mu_n(L))$ condition (2) in 4.3 can be written as

$$\mathrm{h}(G, \mu_n(L)) := \frac{|\hat{\mathrm{H}}^0(G, \mu_n(L))|}{|\hat{\mathrm{H}}^1(G, \mu_n(L))|} = \frac{n}{|G|}\,,$$

$n = \exp(G)$. Since for G cyclic and for the finite G-module $\mu_n(L)$, the quotient $\mathrm{h}(G, \mu_n(L))$ (which is called the Herbrand quotient) is always 1, we get Theorem 4.4 in a more conceptual way. Let us also mention the classical description of the cohomology group $\hat{\mathrm{H}}^1(G, \mu_n(L)) = \mathrm{H}^1(G, \mu_n(L))$ as

$$\hat{\mathrm{H}}^1(G, \mu_n(L)) = L^{\times^n} \cap K^\times / K^{\times^n}$$

derived from the exact sequence $1 \to \mu_n(L) \to L^\times \xrightarrow{n} L^{\times^n} \to 1$ and $\hat{\mathrm{H}}^1(G, L^\times) = 1$.

If $L|K$ is an extension of *finite* fields with $|K| = q$ and $|L| = q^n$ then $|\mu_{\mathrm{er}(n)}(K)| = \mathrm{er}(n)$ is equivalent with $q \equiv 1 \bmod \mathrm{er}(n)$. Of course, this condition implies $q^n \equiv 1 \bmod n$, i.e. $|\mu_n(L)| = n$. Theorem 4.4 has therefore the following corollary which can also be proved more directly.

Corollary 4.6. *An extension $L|K$ of finite fields of degree n with $q = |K|$ has a unitary grading if and only if $q \equiv 1 \bmod \mathrm{er}(n)$. In this case, the grading is a co-Galois grading with cyclic grading group and in particular essentially unique.*

Example 4.7. A cyclotomic field $\mathbb{Q}[\zeta_n]$ over $\mathbb{Q}$ can have a co-Galois grading only in the case $\mathrm{er}(\varphi(n)) \leq 2$ which implies $n|24$. In this case it has a co-Galois grading for trivial reasons (cf. also [1, Corollary 7.4.5]).

A little bit more complicated is the problem to determine the n for which $\mathbb{Q}[\zeta_n]|\mathbb{Q}$ has a unitary (not necessarily co-Galois) grading. *This is the case exactly for*

$$n = 2^\alpha \cdot 3^\beta,\ \alpha \in \mathbb{N},\ \beta \in \{0, 1\}.$$

To see this, one can use the following strategy (for a more detailed account see [5]): Let $L := \mathbb{Q}[\zeta_n]$ be a cyclotomic field which is unitarily D-graded over $\mathbb{Q}$. First consider the case that $n = p^\alpha$ is a prime power. For $p = 2$ there is nothing to prove, so let $p \geq 3$. By considering roots of unity one gets $(p^\alpha - p^{\alpha-1})|2p^\alpha$ which yields $p = 3$. Because the cyclic extension $\mathbb{Q}[\zeta_9]|\mathbb{Q}$ contains the real subfield $\mathbb{Q}[\zeta_9] \cap \mathbb{R}$ of degree 3 over $\mathbb{Q}$ we get $n = 3$.

Now we treat the general case. We can assume that n is even, $n > 2$ and $\varphi(n)|n$. We show that $\varphi(n)$ has to be a power of 2, i.e. $n = 2^\alpha p_1 \cdots p_r$ with Fermat primes p_j, $j = 1, \ldots, r$. Assume there is an odd prime divisor p of $\varphi(n)$. Then there exists a subgroup $\tilde{D}$ of D of order p and $\mathbb{Q}[\zeta_p] \subseteq L_{\tilde{D}}$. But this is a contradiction. Hence the grading group D is a 2-group and moreover $\exp(D) \leq 2^\alpha$. Now let $D = D_1 \times \cdots \times D_s$ be a decomposition of D into cyclic groups. Then the subfields L_{D_j}, $j = 1, \ldots, s$, are linearly disjoint over $\mathbb{Q}$. Hence D has to be of the form $D \cong \mathbb{Z}_{2^e} \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ with $2^e = \exp(D)$. This yields also $\exp(\mathrm{G}(L|\mathbb{Q})) \leq \exp(D)$.

If $\alpha = 1$ we get obviously $n = 6$ and for $\alpha = 2$ one easily checks that $n = 4$ or $n = 12$. Now let $\alpha \geq 3$. By comparing the Galois group

$$\mathrm{G}(L|\mathbb{Q}) = (\mathbb{Z}/\mathbb{Z}n)^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_{p_1-1} \times \cdots \times \mathbb{Z}_{p_r-1}$$

and the grading group D one finds that $n = 2^\alpha(\cdot 3) \cdot 5$ (the factor 3 is optional) and $\exp(D) = 2^\alpha$ is the only critical case. Then we consider the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}[\zeta_{2^\alpha}] \subseteq L_{\mathbb{Z}_{2^\alpha}} \subseteq L$. By Galois theory we see that $L_{\mathbb{Z}_{2^\alpha}} \cap \mathbb{Q}[\zeta_5] = \mathbb{Q}[\sqrt{5}]$. Hence $E := \mathbb{Q}[i, \sqrt{2}, \sqrt{5}] \subseteq L_{\mathbb{Z}_{2^\alpha}}$ and $\mathrm{G}(E|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. But this is a contradiction to $\mathrm{G}(L_{\mathbb{Z}_{2^\alpha}}|\mathbb{Q}) \cong \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_4$.

References

[1] T. Albu. *Cogalois Theory.* New York Basel, 2002.

[2] A. Besicovitch. On the linear independence of fractional powers of integers. *J. London Math. Soc.*, 15:3–6, 1940.

[3] E. C. Dade. Group-graded rings and modules. *Math. Z.*, 174:241–262, 1980.

[4] C. Greither and D. K. Harrison. A Galois correspondence for radical extensions of fields. *J. Pure Appl. Algebra*, 43:257–270, 1986.

[5] A. Kaid. Unitär-graduierte Körpererweiterungen. Diplomarbeit Bochum, 2004.

[6] M. Kneser. Lineare Abhängigkeit von Wurzeln. *Acta Arith.*, 26:307–308, 1975.

[7] G. Scheja and U. Storch. *Lehrbuch der Algebra, Teil 2.* Teubner, 1988.

[8] A. Schinzel. On linear dependence of roots. *Acta Arith.*, 28:161–175, 1975.

[9] C. L. Siegel. Algebraische Abhängigkeit von Wurzeln. *Acta Arith.*, 21:59–64, 1972.

[10] D. Stefan. Cogalois extensions via strongly graded fields. *Comm. Algebra*, 27:5687–5702, 1999.

Holger Brenner (h.brenner@shef.ac.uk), Almar Kaid (a.kaid@shef.ac.uk)
Department of Pure Mathematics, University of Sheffield, Hicks Building, Hounsfield Road, Sheffield S3 7RH, United Kingdom.

Uwe Storch (Uwe.Storch@ruhr-uni-bochum.de)
Fakultät für Mathematik der Ruhr-Universität Bochum, Universitätsstraße 150, D-44801 Bochum, Germany.